AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method of windowed backward key generation, comprising:

[[a)]] providing, by a computer system, information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series ~~and wherein said information is derived from at least one of said limited number of previous key in said series~~;

[[b)]] generating, by the computer system, a key in the series, based at least in part on said information provided to said user;

[[c)]] providing, by the computer system, said generated key in the series to the user[[; and]] to allow a determination of

~~d) said user determining~~ at least one key in the limited number of previous keys in the series by applying said information to said generated key in the series ~~provided to the user~~.

2. (Currently Amended) The method of Claim 1, wherein [[said a)]]providing the information comprises providing a key rotation element that is forward rotatable by said user but is not backward rotatable.

3. (Currently Amended) The method of Claim 1, wherein [[said a)]]providing the information comprises providing to the user a key rotation exponent that is used to determine a previous key in the series from a later key in the series by exponentiating said later key by said key rotation exponent.

4. (Currently Amended) The method of Claim 2, further comprising:

[[e1)]] generating, from the key rotation element, a new key rotation element;

[[e2)]] generating a new key based, in part, on said new key rotation element; and

[[e3)]] distributing said new key to non-revoked users.

5. (Currently Amended) The method of Claim 1, wherein ~~said a) further~~ providing the information comprises providing a secret share and a key rotation catalyst to said user, wherein said secret share and said key rotation catalyst allow said user to generate a next key in the series provided sufficient public information is available.

6. (Currently Amended) The method of Claim 5, further comprising:

[[e)]] publishing at least one public share, wherein the next key in the series is determinable based on the key rotation catalyst, the secret share, and the at least one public share.

7. (Original) The method of Claim 5, further comprising revoking a user by publishing a version of the revoked user's secret share.

8. (Currently Amended) A method of windowed backward key rotation, comprising:

[[a)]] providing, by a computer system, to a user a key rotation element and a key (K_i), wherein later versions of the key rotation element are determinable ~~by the user~~ using a predetermined function but previous versions of the key rotation element are not determinable ~~by said user~~using the predetermined function;

[[b)]] generating, by the computer system, a later version of the key (K_{i+n}) based on a later version of the key rotation element, wherein "n" is a positive integer;

[[c)]] providing, by the computer system, to the user the later version of the key (K_{i+n})[[; and]] to allow a determination of

~~d) said user determining~~ a particular version of the key from (K_i-K_{i+n-1}), inclusive, by applying ~~a version~~ one of the later versions of the key rotation element to a given version of the key from (K_{i+1}-K_{i+n}), inclusive, wherein the given version of the key is a later version than the particular version of the key.

9. (Currently Amended) The method of Claim 8, ~~wherein said d) comprises~~further comprising:

[[d1)]] ~~said user~~ determining a later version of said key rotation element from said provided key rotation element ~~provided in said a)~~.

10. (Currently Amended) The method of Claim 9, wherein ~~said d) further comprises:~~

[[d2)]] ~~said user~~ determining the version of the key K_{i+n-1} is performed by applying the one of the later versions ~~version~~ of the key rotation element to the version of the key K_{i+n}.

11. (Currently Amended) The method of Claim 8, further comprising:

[[e1)]] generating a new key rotation element;

[[e2)]] generating a new key based, in part, on said new key rotation element; and

[[e3)]] distributing said new key to non-revoked users.

12.-14. (Cancelled)

15. ((Currently Amended) A method of windowed backward file key generation, comprising:

[[a)]] generating, by a computer system, ~~an initial~~ a file key;

[[b)]] generating, by the computer system, a ~~an initial~~ key rotation exponent, wherein said ~~initial~~ key rotation exponent allows previous versions of the file [[keys]]key to be determined, wherein a first previous version of the file key is computable from the generated file key and the generated key rotation exponent, and a second previous version of the file key earlier than the first version is computable from the first previous version of the key file and a previous version of the key rotation exponent ~~back until a pre-determined version of the file key, but no file keys further back; and~~

~~c) providing said initial file key and said initial key rotation exponent to initial users~~.

16. (Currently Amended) The method of Claim 15, further comprising:

[[d)]] joining a new user by distributing said [[new]]generated file key and said [[new]]generated key rotation exponent to said new user.

17. (Currently Amended) The method of Claim 15, further comprising:

[[d1)]] generating a new key rotation exponent;

[[d2)]] generating a new file key based, in part, on said new key rotation exponent; and

[[d3)]] distributing said new file key to non-revoked users.

18. (Cancelled)

19. (Currently Amended) The method of Claim 15, ~~wherein~~further comprising:

~~said a) further comprises~~ generating a key rotation catalyst; and

~~said c) further comprises~~ providing a secret share and said key rotation catalyst ~~to ones of said initial users~~, wherein said secret share and said key rotation catalyst allow ~~said initial users to generate~~generation of a new version of the file key provided sufficient public information is available.

20. (Currently Amended) The method of Claim 19, further comprising:

[[d)]] publishing a public share, wherein ~~said initial~~ users are able to determine a new version of the file key using their own secret shares, the public shares, the key rotation catalyst, and a previous file key.

21. (Currently Amended) The method of Claim 19, further comprising:

[[d1)]] generating a new key rotation catalyst;

[[d2)]] publishing said new key rotation catalyst;

[[d3)]] generating a new file key based, in part, on said new key rotation catalyst; and

[[d4)]] publishing a revoked user's private share.

22. (New) The method of Claim 8, wherein the predetermined function is a one-way hash function.